

[Company Logo]

[Return Address]

[Return Address]

[Date]

[Insert Recipient's Name]

[Insert Address]

[Insert City, State, Zip]

RE: Important Security Notification
Please read this entire letter.

Dear [Insert customer name]:

We are writing to inform you of a data security incident experienced by Westminster Financial that may have affected your personal information. Westminster takes the privacy and security of your information very seriously and regrets any concern that this incident may cause. We are writing to notify you of this incident and inform you about steps that can be taken to help protect your personal information.

What Happened? On October 8, 2019 someone from outside Westminster had an unauthorized access of the e-mail account of a Westminster employee. Westminster immediately cut-off the unauthorized third-party access to the e-mail account and has changed the password for the e-mail account. The incident was limited solely to the Westminster employee's e-mail account and there have been no further incidents with the e-mail account. The company has continued to investigate the matter since that time with the help of IT professionals. On October 24, 2019, the Company identified that your personal information was contained in a document that was in the subject e-mail account.

What Information Was Involved? The client information included names and account numbers, social security numbers, or drivers' license numbers. Westminster's IT department is unable to determine if the document in the e-mail containing this information was downloaded, accessed and/or viewed during the unauthorized access to the employee's e-mail account.

What We are Doing? Unauthorized access to the subject e-mail account was immediately terminated and the password for the e-mail account was changed. We also implemented enhanced security measures to our e-mail system to help prevent a similar incident from occurring in the future. This incident was reported to the Federal Bureau of Investigation and applicable regulatory and law enforcement authorities. To date, there has been no suspicious activity with any customer accounts and the company is requiring oral verification of any account changes in order to protect client's accounts. Out of an abundance of caution, we are providing you with information about steps you can take to help protect your information.

What Can You Do? We encourage you to take the following steps to protect yourself and your information:

1. **Review Your Account Statements and Credit Reports.** Remain vigilant by reviewing your account statements and credit reports closely. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by requesting your report online at <http://www.annualcreditreport.com>, or by calling toll-free 1.877.322.8228. You may also purchase a copy of your credit report by contacting one of the three national agencies:

Equifax
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374
1.866.349.5191

Experian
www.experian.com
P.O. Box 2104
Allen, TX 75013-0949
1.888.397.3742

TransUnion
www.transunion.com
P.O. Box 2000
Chester, PA 19016-2000
1.833.395.6938

2. **Fraud Alert.** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity with your report and requests that the creditor contact you prior to opening any accounts in your name. Additional information is available at <http://www.annualcreditreport.com>.
3. **Security Freeze.** You may also want to consider putting a security freeze on your credit files. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You will need to provide your name, date of birth, SSN, and address. The security freeze must be placed with each credit reporting agency (contact information above) and there is no charge.

Equifax: <https://www.equifax.com/personal/credit-report-services/credit-freeze/>

Experian: <https://www.experian.com/freeze/center.html>

TransUnion: <https://www.transunion.com/credit-freeze>

4. **Report Suspicious Activity & Obtain More Information.** If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any suspected identity theft to law enforcement (you have the right to obtain and/or file a police report), your state attorney general, and/or the Federal Trade Commission. More information can be found at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1.877.438.4338
<https://www.ftc.gov/>

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us, 1-888-743-0023

For More Information. If you have questions or need assistance, please contact Jessica M. Trunk at 1.937.665.0117.

We take the protection of your personal information very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,